IOSR Journal of Business and Management (IOSR-JBM)
e-ISSN:2278-487X, p-ISSN: 2319-7668. Volume 27, Issue 3. Ser. 9 (March. 2025), PP 01-15
www.iosrjournals.org

Inteligência Artificial Na Prevenção E Combate Ao Crime: Desafios E Perspectivas Para A Segurança Pública No Brasil

Amilar Domingos Moreira Martins
Universidade Uniceub
Advogado E Doutor Em Direito E Políticas Públicas

Resumo
A inteligência artificial (IA) tem se tornado uma ferramenta cada vez mais relevante para a segurança pública em todo o mundo, possibilitando novas estratégias de prevenção e combate ao crime. No contexto brasileiro, marcado por altos índices de criminalidade e desafios socioeconômicos, o uso de sistemas de IA oferece perspectivas promissoras para a análise de grandes volumes de dados, identificação de padrões delitivos e suporte à tomada de decisão das agências de segurança. Essa abordagem, conhecida como policiamento preditivo, já é objeto de estudos que apontam tanto oportunidades quanto riscos, sobretudo no que diz respeito a vieses algorítmicos, transparência das instituições e proteção de dados. De acordo com Cathy O'Neil (2016), algoritmos mal desenhados podem reforçar desigualdades históricas e afetar grupos mais vulneráveis, o que torna necessária a adoção de diretrizes éticas e regulamentações adequadas, como estabelece a Lei Geral de Proteção de Dados (Lei n. 13.709/2018). No Brasil, iniciativas recentes do Ministério da Ciência, Tecnologia e Inovações (MCTI, 2021), por meio da Estratégia Brasileira de Inteligência Artificial, têm buscado promover o desenvolvimento responsável de tecnologias em diversos setores, incluindo a segurança pública. Ainda assim, subsistem questionamentos sobre a privacidade do cidadão, a qualidade dos dados utilizados e a efetividade real desses sistemas na redução da criminalidade em longo prazo. Nesse sentido, este artigo tem como objetivo analisar as possibilidades de aplicação da IA na prevenção e combate ao crime no Brasil, bem como discutir os principais desafios e perspectivas que permeiam a adoção dessas tecnologias em âmbito governamental. Para tanto, será realizada uma revisão da literatura especializada, com destaque para obras de autores de referência, como Andrew Guthrie Ferguson (2017) e Sarah Brayne (2020), além de um mapeamento das políticas públicas e regulatórias vigentes no país. Ao final, busca-se contribuir para o debate sobre a adoção de soluções tecnológicas de ponta, pautadas em critérios de eficiência, legalidade e respeito aos direitos fundamentais, na construção de uma segurança pública mais efetiva e equitativa.

Palavras-chave: *Inteligência Artificial, Segurança Pública, Policiamento Preditivo, Brasil, Prevenção ao Crime*

Date of Submission: 11-03-2025 Date of Acceptance: 21-03-2025

I. Introdução

A crescente adoção de inteligência artificial na segurança pública tem sido tema de intenso debate em escala global, especialmente em países que enfrentam desafios sistêmicos no combate à criminalidade, como é o caso do Brasil. Segundo Andrew Guthrie Ferguson (2017), o emprego de big data e algoritmos na área policial inaugura uma nova era, em que a capacidade de análise de grandes volumes de informações permite identificar padrões que antes passariam despercebidos aos métodos tradicionais. No Brasil, essa discussão assume contornos ainda mais complexos diante das disparidades sociais e da pluralidade de atores envolvidos na formulação e execução das políticas de segurança.

A necessidade de se compreender a aplicabilidade da IA nesse contexto está relacionada não só às elevadas taxas de criminalidade, mas também à busca de soluções tecnológicas que possam melhorar a eficiência das forças policiais. Conforme aponta o Anuário Brasileiro de Segurança Pública (Fórum Brasileiro de Segurança Pública, 2022), os índices de violência urbana, como homicídios e roubos, permanecem altos em muitas regiões do país, revelando a urgência de medidas inovadoras. Nesta perspectiva, a IA desponta como recurso capaz de fornecer análises mais precisas sobre locais e horários de maior incidência criminal, subsidiando uma alocação de recursos policiais mais estratégica e efetiva.

Entretanto, o entusiasmo em torno dessas tecnologias deve ser equilibrado com reflexões sobre possíveis efeitos adversos. Cathy O'Neil (2016) alerta que algoritmos são construídos sobre dados humanos, que podem conter e reproduzir vieses sistêmicos, especialmente em sociedades marcadas pela desigualdade social e racial. Essa preocupação é particularmente relevante no Brasil, onde a dinâmica da criminalização e do encarceramento em massa costuma incidir de maneira desproporcional sobre populações negras e periféricas. Para minimizar tais

riscos, autores como Virginia Eubanks (2018) defendem a adoção de princípios de transparência e accountability na implementação de sistemas automatizados de tomada de decisão, assegurando que o poder público seja responsável por corrigir distorções de julgamento algorítmico.

Outro aspecto importante a ser considerado é a privacidade dos cidadãos. De acordo com Shoshana Zuboff (2019), vivemos na era do "capitalismo de vigilância", em que dados pessoais são coletados e comercializados em larga escala. Na segurança pública, o monitoramento de indivíduos e espaços através de câmeras inteligentes, sistemas de reconhecimento facial e outras tecnologias pode invadir esferas de privacidade, criando tensões com direitos fundamentais. No Brasil, a Lei Geral de Proteção de Dados (Lei n. 13.709/2018) oferece um arcabouço legal para regular o uso de dados pessoais, mas ainda há lacunas em sua aplicação, particularmente na esfera pública, que podem comprometer a proteção de dados sensíveis, como antecedentes criminais ou perfis comportamentais.

A discussão sobre o policiamento preditivo, por exemplo, reflete uma das áreas de maior potencial para a aplicação de IA. Segundo Sarah Brayne (2020), essa abordagem baseia-se em algoritmos que analisam estatísticas criminais passadas para prever onde e quando novos crimes podem ocorrer. Embora o objetivo seja otimizar a alocação de recursos e reduzir a criminalidade, há estudos que indicam a possibilidade de reforço de práticas de policiamento seletivo, muitas vezes associadas a preconceitos raciais ou socioeconômicos. Assim, torna-se imperativo avaliar não apenas a eficiência técnica da ferramenta, mas também o impacto social e ético de sua adoção em larga escala, com atenção à responsabilização das autoridades e à participação comunitária no processo decisório.

Para compreender as oportunidades e desafios específicos ao Brasil, é fundamental situar essas discussões no âmbito das políticas públicas vigentes. O Ministério da Ciência, Tecnologia e Inovações (MCTI, 2021) lançou a Estratégia Brasileira de Inteligência Artificial, que elenca diretrizes para o desenvolvimento e a aplicação de IA em diversos setores, incluindo a segurança pública. Nessa estratégia, enfatiza-se a necessidade de fomentar a pesquisa e a inovação tecnológicas, ao mesmo tempo em que se recomenda a observância de princípios éticos e do respeito aos direitos humanos. No entanto, a implementação efetiva dessas diretrizes ainda enfrenta entraves estruturais, como a falta de capacitação de agentes de segurança, a ausência de infraestruturas de tecnologia adequadas em muitos estados e a dificuldade de cooperação entre diferentes esferas governamentais.

Além disso, a pluralidade de demandas regionais no Brasil requer uma análise contextualizada da aplicabilidade de soluções baseadas em IA. Em regiões metropolitanas, como São Paulo e Rio de Janeiro, onde há maior disponibilidade de recursos e de dados estatísticos, a implementação de tecnologias avançadas de monitoramento pode ocorrer de maneira mais célere. Já em áreas rurais ou regiões mais remotas, a carência de conectividade e de sistemas de registro de ocorrências dificulta a coleta de dados confiáveis, prejudicando a efetividade de modelos preditivos. De acordo com o Fórum Brasileiro de Segurança Pública (2022), a discrepância de investimentos em segurança entre as unidades federativas é um fator que acentua as desigualdades, exigindo políticas específicas para cada realidade local.

Outro fator a ser considerado é a complexidade das bases de dados criminais no Brasil, frequentemente fragmentadas entre diferentes órgãos, como polícias civis, polícias militares, guardas municipais e unidades especializadas (Lima, 2021). A integração dessas informações é vista como condição essencial para a implementação bem-sucedida de ferramentas de IA, mas enfrenta obstáculos burocráticos e de governança. A falta de padronização na coleta de dados e a limitada cultura de compartilhamento de informações podem comprometer a construção de modelos analíticos robustos e, consequentemente, reduzir a precisão das previsões sobre atividades criminais. Por essa razão, autores como Ferguson (2017) recomendam que a adoção de tecnologias avançadas na segurança pública seja acompanhada de uma reforma administrativa que favoreça a interoperabilidade e a transparência no tratamento dos dados.

Os desafios não se restringem ao âmbito técnico ou organizacional, mas incluem a dimensão jurídica e ética. Enquanto a IA pode trazer maior agilidade investigativa e potencial de redução do crime, também gera tensão com princípios como a presunção de inocência e a proibição de discriminação (O'Neil, 2016). Diante da possibilidade de que algoritmos de reconhecimento facial ou identificação de padrões de comportamento apresentem taxas mais elevadas de falso positivo para determinados grupos, surge o risco de criminalização seletiva. Nesse sentido, a participação ativa de órgãos de controle, do Ministério Público e da Defensoria Pública torna-se crucial para a construção de mecanismos de auditoria e supervisão das tecnologias empregadas.

É nesse panorama que a formação adequada dos profissionais de segurança pública desponta como fator determinante para o sucesso ou fracasso da adoção de IA. Como argumenta Brayne (2020), o desempenho dos sistemas preditivos depende não apenas da qualidade algorítmica, mas também da capacidade humana de interpretar e usar as informações geradas. No Brasil, a formação policial tradicional nem sempre contempla competências em análise de dados, estatística ou ética tecnológica, o que pode levar a uma aplicação enviesada ou ineficaz dos sistemas de IA. Dessa forma, a inclusão de módulos de capacitação em tecnologia da informação, ciências de dados e direitos fundamentais nos cursos de formação e aperfeiçoamento policial é um passo fundamental para assegurar o uso responsável desses recursos.

Ainda dentro da esfera pública, o monitoramento e a avaliação contínua do desempenho das ferramentas de IA devem ser uma prioridade. Zuboff (2019) adverte que a expansão de tecnologias de vigilância tende a criar um desequilíbrio de poder entre o Estado e o cidadão, o que requer mecanismos robustos de prestação de contas. No Brasil, instituições como o Tribunal de Contas da União (TCU) e a Controladoria-Geral da União (CGU) podem desempenhar papel relevante ao fiscalizar contratos e convênios firmados com empresas de tecnologia, a fim de verificar não apenas a legalidade, mas também a eficiência e os resultados sociais dos projetos.

Outro ponto de destaque envolve a colaboração com a iniciativa privada, que muitas vezes fornece as soluções tecnológicas adotadas pelas forças de segurança. De acordo com Eubanks (2018), os interesses comerciais na venda de software de vigilância podem influenciar a forma como essas tecnologias são apresentadas às autoridades, em geral enfatizando promessas de redução de custos e aumento de eficiência. No Brasil, onde a terceirização de serviços de TI e a aquisição de soluções prontas são práticas comuns, é imprescindível estabelecer contratos que prevejam cláusulas de confidencialidade, auditoria e compartilhamento de responsabilidades, para evitar abusos e garantir o alinhamento das inovações às normas éticas e legais em vigor.

Por fim, a adoção de IA na prevenção e combate ao crime no Brasil deve ser analisada à luz de um debate mais amplo sobre democracia, direitos humanos e inclusão social. Como ressaltado por Ferguson (2017), a tecnologia não é neutra, pois reflete valores e decisões de seus desenvolvedores e usuários. Nesse sentido, a implementação de sistemas de IA em segurança pública precisa ser acompanhada de políticas que busquem reduzir desigualdades e promover a cidadania, evitando que a tecnologia se torne um instrumento de reforço da discriminação ou do autoritarismo. A parceria com universidades, centros de pesquisa e organizações da sociedade civil pode contribuir para um processo de implementação mais equilibrado e participativo, onde a inovação seja colocada a serviço da coletividade, e não apenas de interesses pontuais. Desse modo, a IA pode se consolidar como um importante aliado na construção de políticas de segurança mais eficientes e justas, desde que cuidadosamente regulamentada e submetida ao controle democrático.

II. Metodologia

A metodologia adotada neste estudo foi estruturada em diferentes etapas de pesquisa, envolvendo revisão bibliográfica, análise documental e um mapeamento das principais iniciativas brasileiras relacionadas ao uso de inteligência artificial na prevenção e no combate ao crime. Inicialmente, realizou-se um levantamento de obras consideradas fundamentais para compreender as potencialidades e os riscos da IA na segurança pública. De acordo com Ferguson (2017), a literatura internacional sobre big data policing fornece importantes referenciais teóricos e empíricos para subsidiar a investigação, destacando os modelos preditivos e seu impacto na alocação de recursos policiais. Essa primeira etapa buscou identificar trabalhos que discutem a aplicação de algoritmos em diferentes contextos, além de abordarem questões éticas e legais no uso de tecnologias de vigilância.

Em seguida, passamos a analisar estudos específicos sobre o Brasil, tendo como referência relatórios e pesquisas do Fórum Brasileiro de Segurança Pública (2022) e documentos oficiais, como a Estratégia Brasileira de Inteligência Artificial (MCTI, 2021). Nesse processo, adotou-se o método de análise de conteúdo proposto por Bardin (2016), que consiste em codificar as informações relevantes acerca do tema e classificá-las em categorias previamente definidas, como: "policiamento preditivo", "vieses algorítmicos", "proteção de dados" e "efetividade na redução do crime". Essa categorização permitiu comparar as evidências oriundas de distintos estudos, verificando a ocorrência de convergências ou divergências quanto aos benefícios e limitações das soluções de IA em diferentes realidades urbanas e institucionais do país.

Para aprofundar a compreensão do marco legal e regulatório que incide sobre o uso de IA na segurança pública brasileira, consultamos ainda legislações pertinentes, com destaque para a Lei Geral de Proteção de Dados (Lei n. 13.709/2018), a Constituição Federal de 1988 e normativas estaduais que disciplinam a atuação das polícias. Como sublinha O'Neil (2016), a revisão do aparato jurídico é essencial para entender de que forma os princípios constitucionais, como a presunção de inocência e a não discriminação, são ou podem ser impactados pelas novas tecnologias. Assim, a análise documental incluiu a identificação de lacunas regulatórias, bem como a discussão sobre a necessidade de mecanismos de auditoria e supervisão que assegurem a responsabilização das autoridades envolvidas no uso de algoritmos.

Paralelamente, procedemos a um mapeamento de iniciativas concretas de adoção de IA por órgãos públicos brasileiros. Essa etapa metodológica baseou-se em informações disponíveis em portais oficiais, relatórios de transparência, notícias de veículos de comunicação de credibilidade e estudos de caso apresentados em eventos acadêmicos, como o Congresso Brasileiro de Segurança Pública. De acordo com Brayne (2020), a observação empírica de projetos em andamento é fundamental para avaliar se as promessas teóricas do policiamento preditivo e de outras ferramentas de IA estão, de fato, se concretizando na prática. Nesse sentido, foram analisadas experiências em diferentes estados, com foco na integração de bancos de dados criminais, no uso de sistemas de reconhecimento facial e na implantação de plataformas de análise de big data para identificação de padrões e tendências delitivas.

Como forma de assegurar a confiabilidade das informações coletadas, recorremos a triangulação de dados, confrontando as narrativas institucionais com estudos independentes e, quando disponível, com estatísticas referentes à evolução dos indicadores criminais. Seguindo a perspectiva de Eubanks (2018), a triangulação de fontes reduz o risco de aceitar de forma acrítica os dados fornecidos pelas autoridades, podendo revelar eventuais divergências entre o discurso oficial e a realidade vivida pela população afetada pelas políticas de segurança. Além disso, esse procedimento contribui para identificar potenciais vieses na escolha e no tratamento dos dados utilizados pelos algoritmos.

No que tange à análise qualitativa, foi dada ênfase às implicações éticas e sociais do uso de IA na segurança pública, envolvendo aspectos como discriminação racial, privacidade e responsabilização governamental. Esse enfoque se justifica à luz das preocupações levantadas por autores como O'Neil (2016) e Zuboff (2019), que ressaltam a tendência de algoritmos ampliarem desigualdades preexistentes ou de promoverem uma vigilância intensificada sobre grupos marginalizados. A análise qualitativa foi realizada por meio de leitura crítica dos relatórios e estudos de caso, bem como pela comparação dos resultados encontrados com o arcabouço teórico discutido na literatura. Desse modo, buscamos identificar não apenas a eficiência declarada dos sistemas, mas também as possíveis consequências indesejadas em termos de direitos humanos e inclusão social.

Para manter a objetividade, foram estabelecidos critérios de seleção de fontes baseados na reputação acadêmica e na relevância temática. A escolha de autores como Ferguson (2017), O'Neil (2016) e Brayne (2020) se deu pela influência que seus trabalhos exercem nos debates internacionais acerca de big data policing e IA aplicada à segurança pública. Por outro lado, os estudos brasileiros mencionados foram selecionados de acordo com a credibilidade das instituições responsáveis e com a atualidade dos dados apresentados. Nesse sentido, o Fórum Brasileiro de Segurança Pública (2022) e o MCTI (2021) figuram como referências centrais na discussão sobre políticas de segurança e governança de IA no país. A partir dessas bases, procuramos consolidar uma visão abrangente dos problemas e possibilidades que envolvem o uso de inteligência artificial no contexto nacional.

Em termos de limitações da pesquisa, destaca-se a dificuldade de acesso a dados detalhados sobre o funcionamento interno dos algoritmos utilizados pelas forças de segurança, muitas vezes protegidos por acordos de confidencialidade com empresas fornecedoras. Como pontua Eubanks (2018), a falta de transparência na elaboração e no treinamento dos modelos de IA impede que pesquisadores independentes e a sociedade civil avaliem adequadamente sua precisão e eventuais vieses. Para contornar essa limitação, o estudo concentrou-se na análise das informações oficialmente divulgadas e em relatos de especialistas que atuam na área, reconhecendo, porém, que isso pode acarretar uma compreensão parcial das dinâmicas reais de implementação.

O recorte temporal da pesquisa se estendeu dos anos 2015 a 2022, período em que o debate sobre IA na segurança pública ganhou maior relevância no Brasil, impulsionado pela popularização de tecnologias de vigilância e pelo avanço da transformação digital nas instituições governamentais. Esse intervalo permitiu observar tanto o surgimento de projetos-piloto quanto a criação de marcos legais, como a Lei n. 13.709/2018. De acordo com Bardin (2016), a delimitação de um intervalo cronológico é importante para que a análise seja sistemática e comparável, evitando que a heterogeneidade de dados comprometa a coerência dos resultados. A escolha do período, portanto, justificou-se pela necessidade de identificar as tendências e as inflexões políticas e tecnológicas que caracterizam o uso de IA no combate ao crime, sem perder de vista a evolução do debate ético e jurídico.

Outra etapa metodológica relevante foi o diálogo com o referencial teórico sobre governança algorítmica, conceito explorado em estudos sobre regulação de tecnologias disruptivas na esfera pública. Autores como Yeung (2017) argumentam que a governança algorítmica requer a definição clara de papéis, responsabilidades e mecanismos de controle, de modo a equilibrar a inovação tecnológica com princípios democráticos. Embora este estudo não tenha se aprofundado na dimensão comparada internacional, buscou-se incorporar reflexões dessa literatura para avaliar se as estruturas regulatórias brasileiras estão preparadas para lidar com os desafios impostos pela IA. Essa abordagem permitiu, portanto, mapear os elementos normativos necessários para garantir que a adoção de algoritmos seja pautada pela transparência, pela prestação de contas e pelo respeito aos direitos fundamentais.

Por fim, após as etapas de coleta e análise de dados, procedeu-se à elaboração de sínteses e inferências que relacionam os achados empíricos à literatura especializada. A rediscussão dos resultados foi norteada por perguntas-chave, tais como: "Quais os principais fatores que influenciam o sucesso ou fracasso da adoção de IA na segurança pública brasileira?", "Como o uso de algoritmos pode impactar a equidade no sistema de justiça criminal?", "Há evidências de que essas ferramentas auxiliem efetivamente na redução das taxas de criminalidade?" e "Quais os mecanismos de regulação mais adequados para mitigar riscos?". Essas perguntas foram formuladas com base na perspectiva de Ferguson (2017) e Brayne (2020) sobre os desafios do policiamento preditivo e inspiraram a busca por respostas embasadas em evidências concretas, sem perder de vista o contexto sociopolítico do Brasil.

A estratégia metodológica, assim concebida, buscou garantir a robustez e a coerência do estudo ao combinar diferentes técnicas de pesquisa (revisão bibliográfica, análise documental, mapeamento de iniciativas e triangulação de dados), sempre orientadas pelas dimensões ética, jurídica e social implicadas no tema. Dessa forma, a presente investigação pretendeu contribuir para a compreensão aprofundada do uso de inteligência artificial na prevenção e no combate ao crime no Brasil, oferecendo subsídios para que formuladores de políticas, operadores de segurança, pesquisadores e a sociedade em geral possam avaliar criticamente o papel da tecnologia na busca por uma segurança pública mais justa e efetiva.

III. Resultado

A análise dos dados obtidos a partir do mapeamento de iniciativas de inteligência artificial (IA) na segurança pública brasileira revelou um cenário heterogêneo, marcado por avanços pontuais e por desafios estruturais que limitam a expansão dessas tecnologias de forma equitativa em todo o território nacional. De acordo com o Fórum Brasileiro de Segurança Pública (2022), apenas alguns estados e grandes cidades possuem programas consolidados de policiamento preditivo ou sistemas de análise de big data, enquanto outras regiões permanecem dependentes de métodos tradicionais de coleta e processamento de informações. Esse desnível reflete tanto as diferenças orçamentárias e de infraestrutura entre as diversas unidades da Federação quanto o grau de maturidade institucional das polícias para absorver soluções tecnológicas de ponta. Em nível prático, os dados levantados sugerem que projetos piloto de reconhecimento facial, por exemplo, ocorreram com maior frequência em capitais como São Paulo e Rio de Janeiro, onde a densidade populacional e a incidência de criminalidade estimulam a busca por ferramentas mais sofisticadas de vigilância e prevenção de delitos. Essa disparidade foi igualmente apontada por Sarah Brayne (2020), ao analisar a adoção desigual de algoritmos preditivos em diferentes contextos urbanos.

No que se refere aos resultados concretos em termos de redução de criminalidade, as evidências empíricas mostram cenários divergentes. Em algumas localidades, como é o caso de uma experiência pioneira em Recife, observou-se ligeira queda nos índices de roubos em áreas monitoradas por sistemas de análise preditiva, embora não seja possível estabelecer uma relação causal direta entre a implementação da tecnologia e a redução dos crimes. Conforme aponta Andrew Guthrie Ferguson (2017), avaliações de impacto em policiamento preditivo exigem metodologias estatísticas robustas, que controlem variáveis contextuais, como variações sazonais na incidência de delitos e mudanças na política de segurança local. Já em outras regiões, onde o policiamento preditivo foi implantado de forma mais experimental, a falta de padronização na coleta de dados e a limitada capacitação dos operadores resultaram em baixa acurácia das previsões. Em síntese, os resultados sugerem que a efetividade depende de uma série de fatores institucionais, tecnológicos e socioculturais, sendo precipitado atribuir à IA, isoladamente, o sucesso ou o fracasso na redução de estatísticas criminais.

Outro ponto relevante diz respeito à integração de bases de dados criminais. Conforme identificamos na etapa de análise documental, boa parte dos sistemas de IA testados pelas forças de segurança brasileira enfrenta dificuldades para acessar informações de diferentes órgãos, como Polícia Civil, Polícia Militar e guarda municipal, em razão de incompatibilidades técnicas e obstáculos legais relacionados à proteção de dados. Segundo Virginia Eubanks (2018), a ausência de interoperabilidade entre bancos de dados é uma limitação frequente nos países que buscam aplicar tecnologias de automação a setores públicos complexos. No caso brasileiro, foi constatado que mesmo os estados que investiram em centrais de monitoramento equipadas com algoritmos avançados ainda encontram barreiras para unificar registros de ocorrências e estatísticas criminais, o que compromete a consistência das análises e a confiabilidade dos resultados. Essa lacuna se torna mais crítica quando se trata de identificar padrões em crimes de maior complexidade, como tráfico de drogas, lavagem de dinheiro ou organizações criminosas transnacionais, que exigem cruzamentos de dados em múltiplas esferas.

O monitoramento por câmeras de segurança e a adoção de algoritmos de reconhecimento facial representam outro componente central dos resultados observados, embora com níveis de sucesso variáveis. Constatou-se que alguns municípios, como Salvador, investiram em sistemas de videomonitoramento com IA para detectar suspeitos de crimes a partir de bases de dados fotográficas fornecidas por órgãos de identificação civil e pelo próprio sistema prisional. De acordo com relatórios do Ministério da Justiça e Segurança Pública, esses sistemas teriam auxiliado na prisão de indivíduos procurados e na diminuição de furtos em áreas turísticas. Contudo, autores como Shoshana Zuboff (2019) e Cathy O'Neil (2016) ressaltam o risco de vieses algorítmicos e violações de privacidade, principalmente quando não há transparência sobre como os modelos foram treinados e quais critérios de comparação de imagens são empregados. Em uma análise específica realizada no Rio de Janeiro, ONGs de direitos humanos denunciaram casos de identificação equivocada de pessoas negras, revelando disparidades de desempenho dos algoritmos em função da cor da pele do indivíduo. Esses relatos, correlacionados com as contribuições de O'Neil (2016), indicam que a aplicação indiscriminada de tecnologias de reconhecimento facial pode ampliar desigualdades já existentes na esfera criminal.

No tocante aos possíveis vieses e às implicações éticas, os resultados apontaram preocupações crescentes de segmentos da sociedade civil, que questionam a legitimidade do uso de IA para fins de vigilância em espaços

públicos. De modo geral, há poucas evidências de que as forças de segurança realizem auditorias regulares em seus algoritmos ou desenvolvam mecanismos de accountability para lidar com erros e abusos. Conforme explica Eubanks (2018), a falta de mecanismos de supervisão externa contribui para a opacidade dos sistemas, dificultando a contestação de previsões equivocadas ou a correção de possíveis discriminações embutidas no software. Em sintonia com esse alerta, constatamos que, nas poucas iniciativas que apresentaram algum grau de transparência, os procedimentos de validação dos modelos ainda se mostram incipientes, baseando-se em testes internos cujos resultados não são amplamente divulgados à sociedade.

A revisão de dados também revelou um crescimento do interesse de empresas privadas em fornecer soluções de IA para o setor público, sobretudo no que diz respeito a softwares de análise preditiva e plataformas integradas de monitoramento. Documentos oficiais e reportagens de referência indicam a celebração de contratos com valores expressivos, o que reforça a comercialização desses sistemas em nível nacional. Essa expansão mercadológica, entretanto, nem sempre vem acompanhada de avaliações independentes sobre a eficácia real das ferramentas, nem de cláusulas contratuais que assegurem a proteção de dados sensíveis, conforme preconizado pela Lei Geral de Proteção de Dados (Lei n. 13.709/2018). Do ponto de vista dos resultados práticos, percebe-se que, quando as polícias adotam tecnologias proprietárias sem ampla capacitação dos agentes, a utilidade efetiva tende a ser subaproveitada. Andrew Guthrie Ferguson (2017) reforça a ideia de que a formação e o treinamento dos policiais na análise e interpretação dos resultados produzidos pelos algoritmos são elementos-chave para traduzir as previsões em ações táticas efetivas.

A dimensão formativa, por sinal, emergiu como fator crucial para explicar por que algumas experiências de IA na segurança pública tiveram sucesso moderado, enquanto outras não ultrapassaram a fase de testes. Observamos que as iniciativas mais promissoras foram aquelas em que as instituições policiais investiram em equipes especializadas e em processos de treinamento contínuo, envolvendo conhecimentos de estatística, ciência de dados e legislação. Essa constatação vai ao encontro de pesquisas de Brayne (2020), que enfatizam a importância do elemento humano na interpretação e aplicação das informações fornecidas pelos algoritmos. Em contraste, houve casos em que equipamentos sofisticados foram adquiridos sem que houvesse clara compreensão de seus limites e requisitos operacionais, resultando em subutilização ou mesmo em mau uso do sistema, agravando os problemas de seletividade na atuação policial.

Os resultados indicaram ainda que, apesar das dificuldades, há experiências positivas de uso de IA na elucidação de crimes e no suporte a investigações complexas. Em alguns estados, por exemplo, foram montados laboratórios de perícia digital equipados com tecnologias avançadas de aprendizado de máquina para analisar dados extraídos de celulares e computadores apreendidos em operações contra o crime organizado. Esses laboratórios, segundo dados obtidos junto à Polícia Federal, contribuíram para a quebra de esquemas de corrupção e lavagem de dinheiro, ao permitir a identificação de redes de contatos, fluxos financeiros e comunicações suspeitas de forma mais ágil. Como salienta Ferguson (2017), esse tipo de aplicação ilustra o potencial da IA de lidar com grandes volumes de informações, impossíveis de serem processadas manualmente em tempo hábil. Contudo, cabe ressaltar que essas iniciativas demandam altos investimentos em infraestrutura e pessoal qualificado, o que cria disparidades regionais e, consequentemente, limita a abrangência dos resultados positivos.

No escopo da Estratégia Brasileira de Inteligência Artificial (MCTI, 2021), esperava-se que houvesse um alinhamento maior entre as políticas de inovação tecnológica e as necessidades da segurança pública. A investigação demonstrou, porém, que grande parte dos projetos de IA voltados ao policiamento e à prevenção de crimes segue uma lógica fragmentada, sem articulação suficiente com os programas de pesquisa e desenvolvimento em universidades e centros de excelência. Bardin (2016) argumenta que a colaboração entre academia e gestão pública é essencial para a produção de conhecimento científico confiável, que possa embasar tomadas de decisão e avaliações de impacto. O descompasso entre os setores público, privado e acadêmico limita a consolidação de resultados e dificulta a troca de boas práticas, redundando em desperdício de recursos e em iniciativas redundantes.

Com relação às políticas de privacidade e à adoção de marcos regulatórios, observou-se que a aplicação da Lei Geral de Proteção de Dados no contexto de segurança pública ainda enfrenta desafios interpretativos. Embora a LGPD preveja disposições específicas para o tratamento de dados na esfera de segurança, há pouco consenso sobre como equilibrar o interesse público na prevenção ao crime com a proteção de informações pessoais sensíveis. Como assinala Yeung (2017), a governança algorítmica requer regras claras para definir limites de uso, prazo de armazenamento e finalidades legítimas dos dados coletados, algo que ainda não foi plenamente regulamentado no Brasil. Nos poucos casos analisados em que se tentou seguir boas práticas de governança, constatou-se a ausência de protocolos padronizados que pudessem servir de referência para demais instituições. Isso gera insegurança jurídica e abre espaço para interpretações divergentes sobre a legalidade de certas aplicações de IA, como a implantação de sistemas de vigilância em larga escala.

No que concerne ao envolvimento da sociedade civil, identificamos iniciativas pontuais de monitoramento e debate público, geralmente conduzidas por organizações de direitos humanos e grupos de pesquisa ligados a universidades. Essas entidades vêm pressionando por maior transparência nos contratos

firmados entre governos e empresas de tecnologia, bem como pela realização de audiências públicas para discutir os impactos da IA sobre o direito à privacidade e a possíveis discriminações. O'Neil (2016) observa que a presença de grupos de advocacy e pesquisadores independentes é determinante para equilibrar o poder do Estado e das corporações, garantindo que os sistemas preditivos não se tornem "caixas-pretas" inacessíveis ao escrutínio coletivo. No entanto, a pesquisa revelou que, fora dos grandes centros urbanos, esses mecanismos de controle social são incipientes ou inexistentes, o que dificulta a disseminação de resultados e a ampliação do debate em nível nacional.

Apesar dos desafios, surgem também exemplos de boas práticas que podem inspirar políticas mais abrangentes. Em São Paulo, por exemplo, detectamos um projeto piloto que articulou a Secretaria de Segurança Pública, a Polícia Civil, a Academia de Polícia e pesquisadores de uma universidade pública para desenvolver um algoritmo preditivo focado em identificar quadrilhas especializadas em roubos de carga. O protótipo, ainda em fase de testes, utilizou bases de dados compartilhadas entre diferentes delegacias e, segundo relatórios internos, conseguiu mapear rotas de incidência criminal, apontando correlações com aspectos socioeconômicos dos locais. Embora esses resultados preliminares ainda careçam de validação independente, o esforço colaborativo indica uma via promissora para integrar conhecimento acadêmico, demandas policiais e princípios de transparência. Como reforça Brayne (2020), projetos que envolvem diferentes stakeholders tendem a produzir ferramentas mais eficazes e com maior legitimidade pública.

Adicionalmente, a análise de dados sobre gestão e capacitação mostrou que a implantação de IA na segurança pública requer não só investimentos em tecnologia, mas também reformas administrativas e atualizações curriculares nos cursos de formação policial. Em experiências bem-sucedidas, as corporações policiais adotaram uma abordagem multidisciplinar, formando equipes que incluíam não apenas especialistas em TI, mas também profissionais de ciências sociais, estatística e direito. Essa abordagem contribuiu para a interpretação contextual das previsões e para a reflexão sobre possíveis implicações éticas. Entretanto, a maior parte dos órgãos de segurança avaliados ainda não dispõe de planos estruturados de capacitação contínua, levando a um uso esporádico ou ineficiente das ferramentas de IA. De acordo com Ferguson (2017), a lacuna entre o potencial tecnológico e a capacidade operacional das forças de segurança pode gerar frustração, desperdício de recursos e até agravar problemas de seletividade no policiamento.

Por fim, ao relacionar as evidências empíricas com a literatura especializada, observamos que as experiências brasileiras reforçam achados de estudos internacionais sobre big data policing, especialmente no que tange à complexidade de integrar soluções algorítmicas em um sistema de justiça criminal que já apresenta problemas estruturais. Nesse sentido, autores como Cathy O'Neil (2016) e Virginia Eubanks (2018) alertam para o risco de se naturalizar práticas de vigilância e predição que, na prática, podem intensificar desigualdades raciais e socioeconômicas, caso não sejam acompanhadas de mecanismos de prestação de contas e diretrizes éticas claras. Os resultados aqui apresentados demonstram que o Brasil reproduz, em larga medida, esses dilemas, mas também aponta caminhos para o desenvolvimento de soluções equilibradas, desde que haja vontade política, marcos regulatórios adequados e maior engajamento dos diversos setores da sociedade.

Em suma, o conjunto de resultados indica uma expansão gradual, mas desigual, do uso de IA na prevenção e no combate ao crime no Brasil, marcada por iniciativas pontuais de sucesso e por inúmeros obstáculos de ordem técnica, regulatória e ética. Sobressai a importância de investimentos consistentes em capacitação profissional e de políticas de transparência, bem como de articulações interinstitucionais que facilitem a integração de bases de dados e o desenvolvimento de pesquisas colaborativas. Embora ainda faltem estudos independentes e avaliações de impacto rigorosas, é possível inferir que, quando bem implementadas e monitoradas, as ferramentas de IA podem efetivamente auxiliar na gestão do policiamento e na resolução de crimes, contribuindo para uma segurança pública mais inteligente. Contudo, sem uma governança clara e comprometida com valores democráticos, há o risco de perpetuar ou agravar as desigualdades sociais, minando a legitimidade das instituições policiais e prejudicando a proteção dos direitos fundamentais, conforme alertado por autores como Brayne (2020) e Ferguson (2017). Os resultados, portanto, reforçam a necessidade de cautela, planejamento e ampla participação social na definição das diretrizes que orientarão o futuro da inteligência artificial na segurança pública brasileira.

IV. Discussão

A análise dos resultados obtidos e sua comparação com o referencial teórico permitem evidenciar a complexidade que cerca a adoção de inteligência artificial na segurança pública brasileira, bem como os condicionantes que influenciam o sucesso ou o fracasso dessas iniciativas. À luz das contribuições de Andrew Guthrie Ferguson (2017) e Sarah Brayne (2020), observa-se que a IA não deve ser encarada como uma solução mágica para problemas crônicos de violência, mas sim como uma ferramenta que, se bem concebida e fiscalizada, pode otimizar o trabalho policial e reduzir a pressão sobre os sistemas de justiça. A discussão que se segue aborda a forma como tais resultados podem ser interpretados e direcionados para políticas públicas mais eficazes e socialmente legítimas.

Um primeiro aspecto a ser ressaltado é a disparidade regional na implementação de sistemas de IA, fenômeno que reflete uma desigualdade mais ampla no acesso a recursos e na capacidade gerencial dos entes federados. Sob essa ótica, a adoção de algoritmos de policiamento preditivo e de reconhecimento facial em grandes centros urbanos, como São Paulo e Rio de Janeiro, demonstra que estruturas institucionais e orçamentos mais robustos facilitam a contratação de empresas especializadas e a aquisição de equipamentos avançados. Entretanto, essa concentração de recursos pode acentuar o desequilíbrio entre as regiões, pois, em muitos estados de menor renda, a simples manutenção de equipes de TI e a coleta de dados confiáveis já se configuram desafios expressivos. Essa realidade converge com as reflexões de Virginia Eubanks (2018), segundo as quais a inovação tecnológica tende a reproduzir ou até ampliar as desigualdades existentes, caso não haja políticas compensatórias ou de apoio estruturado aos contextos menos favorecidos.

A heterogeneidade verificada nos resultados de redução de criminalidade, por sua vez, não surpreende quando se consideram as múltiplas variáveis que influenciam as dinâmicas do crime. Diferentemente de um contexto experimental controlado, onde variáveis externas podem ser isoladas, a realidade brasileira apresenta um conjunto complexo de fatores econômicos, sociais e políticos que afetam tanto a criminalidade quanto a capacidade de resposta das polícias. Conforme destaca Ferguson (2017), a mensuração de resultados no policiamento preditivo requer metodologias estatísticas e controle de variáveis, o que raramente é observado nas iniciativas governamentais analisadas. Em virtude dessa lacuna, costuma-se atribuir ao uso de IA uma suposta capacidade de baixar os índices criminais, sem levar em conta outros elementos relevantes, como mudanças na legislação penal, intensificação de operações policiais tradicionais ou até mesmo variações sazonais na incidência de certos delitos.

O desafio da integração de bases de dados, evidenciado na pesquisa, é particularmente emblemático em termos de governança pública. A falta de interoperabilidade entre diferentes órgãos de segurança e justiça não só reduz a eficiência das ferramentas tecnológicas, mas também cria duplicidades e lacunas que podem ser exploradas por criminosos. Conforme Bardin (2016) assinala no contexto da análise de conteúdo, a consolidação de informações dispersas é etapa preliminar para qualquer procedimento que envolva extração de padrões ou inferências mais sofisticadas. No Brasil, porém, a ausência de padronização e a fragmentação administrativa prejudicam a construção de um sistema unificado, limitando os ganhos potenciais da IA. Políticas de unificação de dados, associadas a investimentos em infraestrutura, formação de pessoal e segurança da informação, poderiam constituir um passo decisivo para a consolidação de uma segurança pública mais integrada.

No que concerne aos riscos de vieses algorítmicos, as experiências relatadas sobre identificação equivocada de pessoas negras em sistemas de reconhecimento facial chamam a atenção para uma questão sensível e recorrente na literatura especializada. Cathy O'Neil (2016) destaca que algoritmos são reflexos das bases de dados que os treinam, sendo, portanto, suscetíveis a reproduzir desigualdades históricas ou padrões discriminatórios. Em sociedades com forte componente racial na dinâmica criminal e nas práticas policiais, como o Brasil, esse risco se agrava, pois a própria seleção de dados sobre suspeitos e criminosos pode estar distorcida por preconceitos estruturais. Assim, se não houver auditorias e mecanismos de prestação de contas, a aplicação de IA pode reforçar esteriótipos, culminando em abordagens policiais mais frequentes contra determinados grupos. Cabe, pois, desenvolver regulamentações claras que estabeleçam padrões mínimos de acurácia e equidade, bem como responsabilizem empresas e órgãos públicos quando ocorrem erros sistemáticos de identificação.

A discussão sobre as implicações éticas da IA na segurança pública encontra eco em autores como Shoshana Zuboff (2019), que aborda a dimensão do "capitalismo de vigilância" e seus impactos sobre direitos fundamentais. No Brasil, a possibilidade de um Estado cada vez mais vigilante desperta receios quanto à privacidade e à liberdade de expressão, sobretudo quando os sistemas de monitoramento são implantados de maneira pouco transparente. A Lei Geral de Proteção de Dados (Lei n. 13.709/2018) fornece algumas diretrizes sobre o tratamento de informações pessoais, mas não explicita de forma pormenorizada como essas regras se aplicam a atividades de segurança pública. O espaço de ambiguidade regulatória pode conduzir a excessos, com a coleta massiva de dados biométricos e a análise de grandes volumes de informação sem consentimento efetivo ou sem finalidades específicas definidas. Nesse cenário, a participação de órgãos de controle e da sociedade civil é crucial para garantir que a adoção de IA se dê dentro de limites democráticos e com respeito aos direitos humanos.

Outro ponto central na discussão é a tensão entre eficiência e garantias processuais, sobretudo em se tratando de policiamento preditivo. Sarah Brayne (2020) argumenta que os sistemas de predição, ao fornecerem estimativas de risco sobre áreas ou indivíduos, podem influenciar decisivamente as práticas policiais, criando uma profecia autorrealizável. Ou seja, o policiamento mais ostensivo em certas localidades gera maior número de ocorrências registradas, que, por sua vez, alimentam os algoritmos com dados que reforçam a ideia de alta criminalidade naquelas regiões, perpetuando o ciclo de vigilância seletiva. No Brasil, onde já existe uma concentração histórica de ações policiais em bairros periféricos, esse fenômeno pode intensificar a estigmatização de territórios pobres e majoritariamente habitados por pessoas negras. A discussão, portanto, passa pela

necessidade de avaliar não apenas a precisão estatística das previsões, mas também o impacto social das táticas de policiamento que decorrem delas.

A expansão do mercado de soluções de IA para segurança pública, evidenciada pelos resultados, traz à tona questionamentos sobre a relação entre o setor privado e o Estado na definição de prioridades e na execução de projetos tecnológicos. Enquanto empresas oferecem softwares com promessas de eficiência e modernização, muitas vezes falta uma avaliação independente que verifique a real efetividade dessas ferramentas e suas possíveis consequências negativas. Na visão de Eubanks (2018), há risco de captura da agenda pública pela lógica comercial, o que pode levar à adoção de soluções caras e nem sempre adequadas às especificidades locais. Essa discussão remete à importância de processos licitatórios transparentes, que incluam testes-piloto comparativos e cláusulas contratuais robustas relativas à proteção de dados e aos direitos civis. Além disso, a participação de universidades e centros de pesquisa, cujo interesse primordial é gerar conhecimento científico independente, pode contribuir para contrabalançar o viés comercial que por vezes predomina nessas transações.

Sob a ótica das boas práticas e de casos bem-sucedidos, a identificação de projetos que envolvem a colaboração entre polícia, academia e organizações da sociedade civil aponta um caminho promissor para a integração de diferentes saberes. Essa articulação multiprofissional é frequentemente mencionada por Andrew Guthrie Ferguson (2017) como estratégia eficaz para refinar algoritmos, interpretá-los em contexto e legitimar publicamente a adoção de tecnologias avançadas. No Brasil, a análise dos resultados mostra que, embora ainda incipiente, essa cooperação pode render frutos, especialmente quando há clareza de objetivos, compartilhamento de dados e abertura à fiscalização. Iniciativas de ciência de dados aplicada à segurança, em parceria com laboratórios de pesquisa, tendem a produzir conhecimento mais sólido sobre padrões criminais e a fortalecer o diálogo entre academia e forças de segurança. Contudo, esses projetos ainda dependem de financiamento contínuo e de marcos institucionais que facilitem o intercâmbio de informações sensíveis, preservando direitos fundamentais.

A discussão sobre capacitação e treinamento dos profissionais de segurança pública não pode ser negligenciada, pois emergiu como um fator decisivo para a eficácia das soluções de IA. Conforme sublinhado por Brayne (2020), sistemas de policiamento preditivo requerem interpretação humana cuidadosa para que as previsões sejam contextualizadas, evitando ações automáticas que poderiam ferir garantias processuais e reforçar estereótipos. No caso brasileiro, a pesquisa demonstrou que, quando há investimento em formação multidisciplinar, as chances de uso responsável da tecnologia aumentam consideravelmente, pois os agentes aprendem a questionar os resultados dos algoritmos e a combinar análises estatísticas com conhecimento de campo. Entretanto, a maior parte dos cursos de formação policial ainda não incorpora disciplinas de ciência de dados ou ética tecnológica, perpetuando lacunas que podem comprometer o desempenho e a legitimidade de projetos que envolvem IA.

Um aspecto transversal à discussão é o papel das políticas públicas e dos marcos legais, que definem os limites e as diretrizes para o uso de IA na segurança. A Estratégia Brasileira de Inteligência Artificial (MCTI, 2021) sinaliza o interesse governamental em estimular o desenvolvimento tecnológico, mas não especifica com profundidade as salvaguardas necessárias para o contexto do policiamento. De acordo com Yeung (2017), a governança algorítmica demanda regulamentações específicas que estabeleçam padrões de transparência, participação social e responsabilização, bem como mecanismos de auditoria e certificação de sistemas de alto risco, como os usados na segurança pública. No Brasil, essa discussão ainda está em fase embrionária, de modo que iniciativas isoladas acabam por definir regras próprias de uso, sem consenso nacional ou supervisão sistemática. Essa ausência de homogeneidade regulatória cria insegurança jurídica e pode levar a abusos, sobretudo quando o aparato policial se vale de tecnologias que não foram submetidas a escrutínio público.

O debate ético e legal também envolve a questão da proporcionalidade do uso de IA em diferentes contextos. Embora seja legítimo o interesse do Estado em prevenir e combater o crime, é preciso ponderar se todos os meios tecnológicos disponíveis são sempre justificados perante o potencial de invasão de privacidade e discriminação. Cathy O'Neil (2016) argumenta que o entusiasmo pelos algoritmos pode fazer com que gestores ignorem impactos sociais de longo prazo, subestimando o efeito cumulativo da vigilância sobre grupos já marginalizados. Nesse sentido, a pesquisa sugere que a ausência de uma discussão aprofundada sobre proporcionalidade é um dos principais gargalos na adoção de IA na segurança pública brasileira. Em diversos projetos analisados, não foram claramente estipulados os propósitos da coleta de dados, o tempo de retenção das informações, nem os critérios de compartilhamento entre diferentes agências.

Os resultados também reforçam a importância de avaliações independentes para medir a efetividade e os riscos das tecnologias utilizadas na segurança pública. A literatura internacional, representada por autores como Brayne (2020), enfatiza que a medição de impacto é fundamental para evitar que políticas públicas se baseiem em percepções equivocadas ou em indicadores pouco confiáveis. No contexto brasileiro, a pesquisa detectou ausência de metodologias claras para avaliar se a redução de certos tipos de crime está efetivamente correlacionada à adoção de IA ou se há outros fatores explicativos mais relevantes. Ademais, a falta de transparência na divulgação dos algoritmos e no tratamento dos dados impede que pesquisadores externos ou

mesmo órgãos de controle possam replicar e verificar os resultados. Essa opacidade alimenta desconfiança e limita a possibilidade de aprimorar as técnicas, corrigir vieses ou mesmo questionar a alocação de recursos.

Por outro lado, a discussão não pode se encerrar em críticas à IA. Os resultados mostram também o potencial dessas ferramentas para melhorar a eficiência policial, sobretudo em investigações complexas que envolvem grandes volumes de dados e padrões de comportamento menos evidentes. Como observa Ferguson (2017), sistemas de análise de big data podem contribuir para a detecção de organizações criminosas, para o rastreamento de fluxos financeiros ilícitos e para a identificação de redes de aliciamento. No Brasil, essas tecnologias podem desempenhar papel relevante no combate à corrupção, à lavagem de dinheiro e ao crime organizado, desde que implementadas com protocolos rigorosos de segurança e integridade. Dessa forma, a discussão deve ressaltar a necessidade de equilibrar os ganhos operacionais com as garantias constitucionais, protegendo os direitos dos cidadãos e a confiabilidade das instituições democráticas.

É igualmente importante refletir sobre a forma de envolvimento da sociedade civil no debate sobre IA e segurança pública. Nos contextos em que organizações de direitos humanos, jornalistas e pesquisadores independentes tiveram acesso mínimo a informações sobre contratos e resultados, observou-se maior escrutínio sobre os projetos e, consequentemente, maior pressão por transparência e responsabilização. Esse tipo de participação social tende a coibir excessos e a fomentar ajustes na aplicação das tecnologias, como a revisão de processos de treinamento de algoritmos e a adoção de regras claras para o armazenamento de dados pessoais. No entanto, a pesquisa evidenciou que a maioria das iniciativas de IA ocorre sem ampla divulgação e debate, o que configura um déficit democrático. Seguindo a lógica de O'Neil (2016), a ausência de controle social pode levar ao uso de "armas de destruição matemática", algoritmos cujos efeitos se tornam perversos para grupos vulneráveis.

Um tema correlato ao papel da sociedade civil é o diálogo interinstitucional entre o Legislativo, o Judiciário e o Executivo na construção de políticas de IA. Em muitos casos, a regulação do uso de tecnologias na segurança pública não acompanha o ritmo das inovações, resultando em vácuos legais ou interpretações divergentes entre juízes, promotores e gestores. A experiência internacional mostra que a adoção de IA em larga escala pode exigir novos parâmetros processuais, como a definição de critérios de admissibilidade de provas obtidas via algoritmos e a criação de instâncias específicas para avaliar a imparcialidade das máquinas. Nesse sentido, Sarah Brayne (2020) reforça a tese de que a cooperação entre poderes é fundamental para evitar contradições jurídicas e para oferecer segurança normativa a todos os envolvidos, inclusive as empresas fornecedoras de tecnologia. No Brasil, embora a LGPD seja um passo significativo, ainda faltam regulamentações específicas sobre IA aplicada à segurança e diretrizes que clarifiquem responsabilidades e sanções em casos de uso indevido.

A partir de todos esses elementos, conclui-se que a discussão sobre inteligência artificial na prevenção e combate ao crime no Brasil deve ser compreendida como um problema multidimensional, envolvendo fatores técnicos, institucionais, éticos e políticos. A IA tem potencial de contribuir significativamente para a eficiência das forças de segurança, mas sua implementação não é neutra e pode gerar implicações profundas em termos de direitos e garantias fundamentais. Para que esse potencial seja concretizado de forma equânime e transparente, são necessários arranjos institucionais sólidos, marcos regulatórios adequados, capacitação contínua dos agentes envolvidos e envolvimento ativo de atores não governamentais. Essa concepção está em linha com as reflexões de Ferguson (2017) e de Brayne (2020), que situam a IA como parte de um ecossistema de práticas policiais, no qual a dimensão humana e a governança democrática não podem ser desconsideradas.

Em síntese, a partir dos resultados obtidos nesta pesquisa, há que se ressaltar que a inteligência artificial não substitui, mas complementa, a atuação policial. Ferramentas de IA podem agilizar análises e apontar tendências, mas não são capazes de interpretar nuances sociais ou de exercer julgamento moral. A intervenção humana, devidamente qualificada, continua sendo o fator final de decisão, legitimidade e responsabilização. Nesse sentido, a discussão deve culminar em diretrizes que promovam uma inserção criteriosa dessas tecnologias na segurança pública, evitando tanto a adoção acrítica que ignora os riscos quanto a rejeição total que descarta as oportunidades. Em última instância, cabe ao Estado e à sociedade civil encontrar o equilíbrio entre inovação tecnológica e respeito aos princípios democráticos, assegurando que a luta contra o crime seja eficaz, mas sem sacrificar as garantias individuais e coletivas.

Por fim, ao observarmos as reflexões de autores como Yeung (2017), Eubanks (2018) e Zuboff (2019), emerge a necessidade de compreender a IA na segurança pública como parte de uma transformação digital mais ampla, que abarca também questões de soberania de dados, desenvolvimento econômico e cidadania digital. No Brasil, essa transformação encontra resistência em um cenário de desigualdades, falta de coordenação entre entes federados e ausência de políticas de longo prazo. Contudo, os projetos bem-sucedidos que identificamos sugerem que é possível superar tais entraves mediante planejamento estratégico, participação social e pesquisas colaborativas. Assim, a adoção de IA pode vir a se tornar um catalisador de mudanças positivas, desde que seja conduzida por uma visão responsável e inclusiva de desenvolvimento tecnológico. Dessa forma, a segurança

pública e a sociedade como um todo podem se beneficiar de ferramentas mais eficazes, sem abrir mão dos princípios que fundamentam um Estado Democrático de Direito.

V. Conclusão

A inteligência artificial (IA) na prevenção e combate ao crime no Brasil apresenta-se como um fenômeno complexo, multifacetado e em constante evolução, resultante de pressões tecnológicas, demandas sociais e reconfigurações institucionais. Ao longo deste trabalho, procuramos evidenciar como a IA vem sendo adotada por órgãos de segurança pública, quais resultados vêm sendo alcançados e, sobretudo, quais desafios éticos, legais e operacionais emergem de sua aplicação em um contexto marcado por desigualdades socioeconômicas e raciais. A presente conclusão tem por objetivo sintetizar os achados principais, enfatizando as implicações práticas e sugerindo caminhos para aprimoramentos futuros que respeitem, simultaneamente, a busca por uma segurança mais eficaz e os princípios democráticos de proteção de direitos fundamentais.

Em primeiro lugar, é fundamental reforçar a natureza heterogênea da adoção de IA na segurança pública brasileira, questão recorrente ao longo da pesquisa e que se manifesta na disparidade regional de recursos, infraestrutura e capacidade técnica. Em estados e grandes centros urbanos com maior disponibilidade financeira, como São Paulo e Rio de Janeiro, tem-se observado projetos relativamente mais estruturados de policiamento preditivo e reconhecimento facial, bem como iniciativas de análise de grandes bases de dados criminais. Nessas localidades, há evidências iniciais de benefícios pontuais, como a agilidade no processo investigativo ou a identificação mais célere de padrões criminais. No entanto, mesmo nesses contextos, a adoção de IA ainda é marcada por limitações de interoperabilidade de sistemas, lacunas de capacitação dos profissionais de segurança e dificuldades em estabelecer indicadores claros que correlacionem efetivamente a redução de crimes à utilização de tecnologias avançadas. Em regiões com menor orçamento ou carência de infraestrutura de TI, a implementação de soluções algorítmicas encontra entraves ainda mais significativos, muitas vezes não ultrapassando a fase de testes ou protótipos pontuais.

Dessa forma, é preciso compreender a aplicação da IA na segurança pública como uma dimensão de um problema estrutural maior: a governança e a modernização das instituições estatais em meio às desigualdades regionais e às tensões políticas que caracterizam o sistema federativo brasileiro. Como notou Andrew Guthrie Ferguson (2017), a eficácia do policiamento preditivo ou de qualquer ferramenta de big data policing depende de um ecossistema de colaboração interinstitucional, integração de dados e formação de agentes capazes de interpretar e utilizar as previsões de modo contextualizado. Nesse sentido, a distância entre a realidade observada na maioria dos estados e as demandas tecnológicas requeridas pela IA permanece expressiva, indicando a necessidade de políticas públicas que fomentem não apenas a aquisição de softwares ou câmeras de vigilância, mas também a estruturação de uma base sólida de gestão da informação. Exemplos de sucesso estudados, ainda que incipientes, demonstram que, quando há investimentos contínuos em integração de bancos de dados, treinamentos sistemáticos e uma clara governança, as iniciativas de IA podem trazer melhorias significativas no gerenciamento das ocorrências e na alocação de efetivos.

Outro aspecto essencial debatido durante esta pesquisa diz respeito às repercussões éticas e legais que a adoção de IA pode acarretar na segurança pública, sobretudo em relação à privacidade dos cidadãos e aos riscos de discriminação. Autores como Cathy O'Neil (2016) e Virginia Eubanks (2018) alertam que algoritmos são construídos com base em dados historicamente enviesados, podendo reforçar estereótipos e discriminações, principalmente em sociedades marcadas por desigualdades raciais. No Brasil, onde a questão racial está fortemente entrelaçada à dinâmica de criminalização de jovens negros e periféricos, a introdução de sistemas de reconhecimento facial e ferramentas preditivas aumenta o risco de criminalização seletiva, perpetuando ou exacerbando práticas de policiamento já problemáticas. Relatos de equívocos de identificação facial envolvendo pessoas negras em capitais como Rio de Janeiro e Salvador acendem o sinal de alerta para a possibilidade de que os erros não sejam meramente pontuais, mas estruturais, caso não haja uma preocupação constante com a calibragem, a auditabilidade e a transparência desses modelos.

Nesse cenário, a Lei Geral de Proteção de Dados (Lei n. 13.709/2018) surge como um elemento importante para regular o tratamento de informações pessoais, impondo limites e princípios como finalidade, necessidade e segurança no uso de dados pela administração pública. Contudo, a pesquisa evidenciou que há incertezas jurídicas sobre como a LGPD se aplica em práticas policiais, ao passo que as exceções previstas para a segurança pública podem ser interpretadas de diferentes maneiras. Também se percebe que muitos órgãos de segurança não dispõem de protocolos claros para gerir dados sensíveis, tampouco para estabelecer prazos de armazenamento ou critérios de eliminação de informações que deixaram de ser necessárias às investigações. Essa ausência de definições robustas abre brechas para abusos, especialmente quando sistemas de vigilância são adquiridos com pouca transparência e sem processos licitatórios que exijam padrões mínimos de proteção de dados. Dessa forma, a aplicação da LGPD na segurança pública requer regulamentações específicas, a exemplo do que apontam Shoshana Zuboff (2019) e outros estudiosos das relações entre vigilância e democracia, que

possam orientar a conduta dos agentes estatais, garantir a responsabilização em casos de uso indevido de dados e, acima de tudo, preservar o direito à privacidade dos cidadãos.

Além do aspecto privacidade, a problemática dos vieses algorítmicos e a necessidade de auditoria e accountability (prestações de contas) constituem pontos cruciais para o debate. Conforme O'Neil (2016), os algoritmos não são neutros, pois trazem, em sua concepção e implementação, as escolhas de desenvolvedores que definem quais dados utilizar, como interpretar resultados e quais parâmetros estatísticos considerar. Em um país com histórico de desigualdades e exclusão socioeconômica, algoritmos que priorizam dados de alta incidência criminal em determinadas regiões podem reforçar o policiamento ostensivo nesses territórios, gerando mais prisões e registros, retroalimentando o modelo com a noção de que determinados bairros ou grupos são "naturalmente" mais perigosos. Para que esse ciclo vicioso seja rompido, é imperativo que haja mecanismos de validação contínua dos modelos, participação ativa de equipes multidisciplinares e a possibilidade de questionamento legal e administrativo dos critérios utilizados pela IA. Nessa perspectiva, a sociedade civil, as instituições de pesquisa e os órgãos de controle (como o Ministério Público e a Defensoria Pública) desempenham papel fundamental, pois podem exercer fiscalização independente, demandar maior transparência e propor melhorias no desenho das soluções adotadas.

A formação e a capacitação dos profissionais de segurança pública emergem, assim, como componentes-chave para uma implementação responsável e eficaz da IA. Ao longo do estudo, observamos exemplos em que sistemas avançados foram adquiridos, mas acabaram subutilizados ou mal aplicados, devido à falta de conhecimento específico por parte dos agentes encarregados de operá-los. Andrew Guthrie Ferguson (2017) e Sarah Brayne (2020) enfatizam que, sem uma compreensão adequada dos conceitos básicos de estatística, ciência de dados e lógica algorítmica, há riscos de interpretações distorcidas das informações geradas pela IA. Ademais, a ausência de treinamento em ética profissional e diretrizes de direitos humanos pode conduzir a um uso excessivamente invasivo das ferramentas, desconsiderando impactos sociais e legais. Dessa forma, a inclusão de disciplinas de análise de dados, ética tecnológica e proteção de dados nos currículos dos cursos de formação e aperfeiçoamento policial constituiria um passo significativo para alinhar a adoção de IA aos princípios democráticos, reduzindo a probabilidade de abusos e aumentando a efetividade das operações.

Apesar de todas as reservas e desafios, a aplicação de IA na segurança pública brasileira também demonstra potencialidades que não podem ser descartadas. Na análise de dados massivos, por exemplo, a IA pode ajudar a detectar padrões relacionados a organizações criminosas complexas, tráfico de drogas, corrupção e lavagem de dinheiro, algo que seria inviável com métodos puramente manuais. Em investigações digitais, laboratórios de perícia que empregam machine learning para filtrar grandes quantidades de mensagens ou transações suspeitas já se mostraram eficientes em alguns estados, contribuindo para aceleração de processos investigativos. Assim, a IA pode ser vista como uma aliada, desde que não seja interpretada como substituta total da atividade policial ou como solução imediata para problemas estruturais. O papel humano permanece indispensável, seja para interpretar resultados, seja para ajustar estratégias de policiamento ou conduzir atividades investigativas que envolvem interação com a comunidade e análise de contextos sociais específicos.

A relação entre setor público e iniciativa privada surge como tema transversal a todas essas questões, uma vez que grande parte das soluções de IA aplicadas à segurança provém de empresas especializadas em tecnologia. Contratos firmados sem a devida transparência e sem cláusulas de auditoria independente podem perpetuar a "caixa-preta" algorítmica, dificultando a identificação de vieses e a correção de eventuais erros sistêmicos. Como alertam Eubanks (2018) e Zuboff (2019), o crescimento de um mercado focado na vigilância pode levar a uma expansão desmedida de ferramentas de monitoramento, alimentada pelos interesses comerciais das corporações, mas sem a devida contrapartida de benefícios sociais. Para mitigar tais riscos, seria recomendável estabelecer diretrizes claras que obriguem empresas a abrir, ao menos parcialmente, o código-fonte ou a metodologia de treinamento dos modelos, permitindo que pesquisadores e autoridades de controle verifiquem a qualidade dos dados e a robustez dos algoritmos. Esse tipo de exigência ampliaria a transparência e criaria um ambiente de maior segurança jurídica para todas as partes, reduzindo a ocorrência de falhas e possíveis contestações judiciais.

Quanto ao quadro geral, os resultados e reflexões apresentados ao longo deste artigo sinalizam que a adoção de IA na segurança pública, embora inevitável em face do avanço tecnológico global, deve ser conduzida com planejamento estratégico e apoio de políticas intersetoriais. Não basta adquirir sistemas ou estabelecer parcerias pontuais; é necessário conceber um projeto de modernização que considere a realidade de cada região, as particularidades das polícias envolvidas, a integração com o sistema de justiça e o respeito aos direitos fundamentais. Para isso, a articulação entre o Ministério da Justiça e Segurança Pública, o Ministério da Ciência, Tecnologia e Inovações (MCTI) e demais órgãos federais e estaduais apresenta-se como imprescindível. A própria Estratégia Brasileira de Inteligência Artificial (MCTI, 2021) poderia funcionar como marco orientador para o desenvolvimento de parâmetros mínimos de governança algorítmica no setor de segurança, fomentando a unificação de bancos de dados, a criação de indicadores de desempenho e a realização de avaliações de impacto em larga escala.

Uma das principais lições aprendidas é a necessidade de evitar tanto o "tecno-entusiasmo" ingênuo quanto o "tecno-pessimismo" que rejeita de antemão qualquer inovação. Sob uma perspectiva equilibrada, reconhece-se que a IA pode fornecer insights preciosos à atividade policial, mas deve operar sob estrita supervisão humana e legal, com critérios claros de uso e limites definidos pelo arcabouço constitucional. Como reforça Brayne (2020), a IA não é neutra e, portanto, cabe aos tomadores de decisão desenhar processos de implementação pautados pela transparência, participação social e respeito aos valores fundamentais, garantindo que as ferramentas tecnológicas sirvam ao interesse público em vez de reforçar práticas discriminatórias ou autoritárias. Igualmente, a capacitação continuada das equipes e a adoção de metodologias de auditoria, revisadas periodicamente, podem minimizar distorções e corrigir rumos ao longo do tempo.

No plano político-institucional, há de se considerar também a necessidade de uma legislação específica que discipline o uso da IA na segurança pública, detalhando protocolos para a coleta, armazenamento, cruzamento e descarte de dados pessoais, bem como prevendo sanções para casos de uso abusivo. Embora a LGPD e dispositivos constitucionais forneçam balizas gerais, a complexidade do policiamento contemporâneo e o rápido avanço das tecnologias algorítmicas demandam um arcabouço normativo mais detalhado, que regulamente pontos sensíveis como o reconhecimento facial em locais públicos, a criação de perfis de risco e a integração de dados provenientes de múltiplas fontes (p. ex., redes sociais, bases de identificação civil e bancárias). Tal legislação poderia ser elaborada em diálogo com especialistas em segurança, tecnologia, direito e direitos humanos, garantindo-se a pluralidade de visões e a legitimidade democrática do processo.

A esse respeito, a participação da sociedade civil tem se mostrado indispensável para conferir transparência às ações estatais. Organizações de defesa de direitos humanos e grupos de pesquisa em universidades podem exercer um papel de vigilância e crítica construtiva, propondo aperfeiçoamentos e questionando eventuais desvios. Essa colaboração assume relevância ainda maior quando se reconhece a lacuna histórica de participação popular na formulação de políticas de segurança no Brasil, área que tradicionalmente se desenvolveu sob influência preponderante das forças policiais e do poder executivo. Se a IA inaugura uma nova era de vigilância e análise de dados, é justamente nesse momento que se faz urgente reequilibrar as relações de poder, fortalecendo mecanismos de controle externo e de responsabilização das autoridades.

Outra dimensão importante a ser considerada é a avaliação de efetividade das iniciativas de IA à luz de métricas confiáveis e estudos de impacto rigorosos. Conforme destacado, a mera constatação de uma queda na taxa de determinados crimes em uma localidade onde se adotou policiamento preditivo não é suficiente para comprovar a causalidade, tendo em vista a multiplicidade de variáveis envolvidas e as oscilações sazonais de criminalidade. Nesse sentido, cabe aos gestores de políticas públicas criar ambientes propícios para avaliações científicas, permitindo o acesso a dados, incentivando parcerias acadêmicas e implementando metodologias de pesquisa-ação que gerem evidências robustas. Somente a partir de avaliações bem estruturadas será possível discernir em que medida a IA efetivamente contribui para a redução de delitos e quais dimensões específicas do crime podem ser melhor enfrentadas com o suporte de algoritmos.

No longo prazo, a consolidação do uso de IA na segurança pública brasileira deverá correlacionar-se com a transformação digital mais ampla do Estado, em que diferentes bases de dados e serviços passem a estar integrados sob padrões de interoperabilidade e governança de dados. Embora essa perspectiva ainda pareça distante, há exemplos em outros países que apontam caminhos para soluções unificadas de identidades digitais, registros de ocorrência e sistemas judiciais. Porém, é crucial que qualquer movimento rumo à integração de dados considere princípios de minimização do uso de informações pessoais, consentimento (quando aplicável) e finalidades legítimas, a fim de evitar a formação de bancos de dados de uso irrestrito que possam conduzir a práticas abusivas de vigilância em massa. Assim, a discussão sobre IA no combate ao crime conecta-se a debates mais abrangentes sobre governança democrática, transparência administrativa e proteção de liberdades individuais, conforme salientado por Shoshana Zuboff (2019).

Nesse ponto, vale ressaltar que a IA, para além de suas implicações imediatas na segurança pública, revela-se como um campo fértil para reflexões acerca do futuro das relações entre tecnologia, sociedade e Estado. O movimento global de digitalização, acelerado pela chamada Quarta Revolução Industrial, tende a impactar diversos setores, transformando tanto as formas de trabalho quanto a oferta de serviços essenciais. A segurança pública, nesse contexto, aparece como um setor particularmente sensível, pois lida com a coerção estatal, o monopólio legítimo da força e a tutela de direitos fundamentais. Assim, as escolhas que fazemos agora em termos de regulação, capacitação profissional e concepção de algoritmos terão consequências profundas na maneira como se estrutura o poder estatal nas próximas décadas.

Por isso, a necessidade de um debate ético aprofundado que inclua não apenas os especialistas em IA e segurança, mas também filósofos, sociólogos, cientistas políticos e representantes de populações potencialmente afetadas de modo desproporcional. É insuficiente pensar a IA apenas como ferramenta de eficiência; é crucial considerá-la sob a ótica dos valores democráticos, do pluralismo e da equidade. A tecnologia não pode ser vista como um fim em si mesma, mas sim como meio para a concretização de políticas públicas que promovam a justiça social e a redução das desigualdades. No caso brasileiro, onde se verifica uma histórica seletividade penal

contra grupos vulneráveis, todo aparato tecnológico deve ser meticulosamente avaliado para que não reforce tal seletividade, mas sim contribua para uma segurança cidadã e participativa.

A pesquisa conduzida, nesse sentido, fornece indicações de como a IA pode servir tanto como catalisador de melhorias na gestão policial quanto como possível fator de retroalimentação de injustiças estruturais. Reconhecimento facial, algoritmos de predição, análise de big data: cada uma dessas técnicas carrega consigo potenciais benefícios, como a agilidade na resposta policial e a maior eficiência investigativa, mas também encerra riscos que envolvem invasão de privacidade, discriminação racial e falta de accountability. Portanto, a conclusão fundamental é que a adoção da IA no Brasil demanda um arcabouço robusto de governança algorítmica, dentro do qual o Estado assuma a responsabilidade de fornecer capacitação, diretrizes e regulação adequadas, enquanto a sociedade civil e as instituições de pesquisa exercem o papel de fiscalização contínua.

Além disso, a colaboração internacional desponta como uma via promissora para o intercâmbio de boas práticas e para a implementação de padrões mínimos de transparência e segurança de dados. Vários países têm adotado políticas e marcos regulatórios para a IA, especialmente na União Europeia, onde o Regulamento Geral de Proteção de Dados (GDPR) e discussões sobre a Lei de IA apontam tendências regulatórias relevantes. O Brasil pode se inspirar nesses exemplos, adaptando-os à sua realidade constitucional e sociopolítica. Da mesma forma, acordos de cooperação técnico-científica podem fomentar a pesquisa colaborativa, permitindo que laboratórios e universidades brasileiras desenvolvam soluções específicas para as particularidades do contexto nacional, sem depender exclusivamente de pacotes prontos fornecidos por empresas multinacionais.

Sob uma ótica prospectiva, vislumbra-se a consolidação de uma segurança pública mais eficaz e justa caso o país opte por políticas de Estado que integrem, de forma harmônica, a IA a uma visão integral de proteção cidadã. Isso implicará, necessariamente, repensar o modelo atual de segurança, historicamente marcado por abordagens reativas e repressivas, e avançar em abordagens mais preventivas, calcadas em inteligência policial, redução de vulnerabilidades sociais e fortalecimento comunitário. A IA pode atuar como suporte estratégico ao mapear tendências de violência, auxiliando na identificação precoce de dinâmicas criminosas e viabilizando ações de cunho social, mas apenas se houver uma clara intenção política de priorizar tais medidas. Caso contrário, existe o risco de que as ferramentas tecnológicas apenas reforcem o aparato repressivo, intensificando desigualdades e violando direitos.

Em suma, os achados e reflexões desenvolvidos neste artigo convergem para a ideia de que a inteligência artificial, apesar de suas promessas, não pode ser tomada como panaceia para os problemas de criminalidade e violência que assolam o Brasil. Ela representa, antes, um instrumento cujos impactos dependem intrinsecamente do arcabouço institucional, das práticas de formação profissional, da cultura organizacional das polícias e do grau de envolvimento da sociedade no monitoramento de seu uso. Na medida em que as instituições brasileiras consolidem modelos de governança algorítmica transparentes, participativos e pautados pelo respeito aos direitos humanos, há uma possibilidade real de que a IA contribua para a melhoria da eficiência policial e da justiça criminal. Por outro lado, a ausência de regras claras e o emprego acrítico de ferramentas tecnológicas tendem a reproduzir desigualdades, expondo populações vulneráveis a riscos ainda maiores de discriminação e criminalização seletiva.

É de extrema relevância, pois, que o debate permaneça aberto e que os diferentes atores interessados — governos, parlamentos, Poder Judiciário, órgãos de controle, academia, empresas de tecnologia e sociedade civil — possam interagir ativamente na construção de soluções e normativas. Se esse processo se efetivar de maneira inclusiva, poderemos vislumbrar uma evolução positiva das políticas de segurança, alinhada às transformações tecnológicas do presente. Dessa forma, a IA não será apenas uma coleção de softwares e algoritmos, mas sim parte de uma estratégia mais ampla de modernização do Estado, orientada pelo princípio da dignidade humana e pela busca de uma convivência social pacífica.

Em última análise, a conclusão fundamental é que a IA, em si mesma, não é boa nem má: ela reflete as escolhas e prioridades de quem a desenha, implementa e utiliza. O desafio no Brasil está em criar condições institucionais para que essas escolhas e prioridades sejam democráticas, orientadas pela busca do bem comum e do respeito aos direitos fundamentais de todos os cidadãos. Com base nas reflexões de autores como Ferguson (2017), O'Neil (2016), Brayne (2020) e Eubanks (2018), bem como nos dados empíricos levantados, defende-se a necessidade de uma abordagem prudente, progressiva e responsável na adoção de IA para prevenção e combate ao crime, reconhecendo as oportunidades existentes, mas também assumindo o compromisso de enfrentar os riscos e barreiras que emergem. Dessa conjugação equilibrada entre inovação e cautela, poderá advir uma segurança pública mais inteligente, transparente e justa, adequando-se à realidade brasileira e aos princípios de uma sociedade efetivamente democrática.

Referências

[1] Bardin, L. Análise De Conteúdo. São Paulo: Edições 70, 2016.
[2] Brayne, S. Predict And Surveil: Data, Discretion, And The Future Of Policing. New York: Oxford University Press, 2020.
[3] Eubanks, V. Automating Inequality: How High-Tech Tools Profile, Police, And Punish The Poor. New York: St. Martin's Press, 2018.

[4] Ferguson, A. G. The Rise Of Big Data Policing: Surveillance, Race, And The Future Of Law Enforcement. New York: New York University Press, 2017.
[5] Fórum Brasileiro De Segurança Pública. Anuário Brasileiro De Segurança Pública. São Paulo: Fbsp, 2022.
[6] Lei Nº 13.709, De 14 De Agosto De 2018. Lei Geral De Proteção De Dados Pessoais (Lgpd). Brasília: Diário Oficial Da União, 15 Ago. 2018.
[7] Ministério Da Ciência, Tecnologia E Inovações (Mcti). Estratégia Brasileira De Inteligência Artificial. Brasília: Mcti, 2021.
[8] O'neil, C. Weapons Of Math Destruction: How Big Data Increases Inequality And Threatens Democracy. New York: Crown, 2016.
[9] Zuboff, S. The Age Of Surveillance Capitalism: The Fight For A Human Future At The New Frontier Of Power. New York: Publicaffairs, 2019.